Minimal Gröbner bases and the predictable leading monomial property

M. Kuijper*and K. Schindelar†‡

May 28, 2010

Abstract

We focus on Gröbner bases for modules of univariate polynomial vectors over a ring. We identify a useful property, the "predictable leading monomial (PLM) property" that is shared by minimal Gröbner bases of modules in $\mathbb{F}[x]^q$, no matter what positional term order is used. The PLM property is useful in a range of applications and can be seen as a strengthening of the wellknown predictable degree property (= row reducedness), a terminology introduced by Forney in the 70's. Because of the presence of zero divisors, minimal Gröbner bases over a finite ring of the type $\mathbb{Z}_{p^r}$ (where p is a prime integer and r is an integer > 1) do not necessarily have the PLM property. In this paper we show how to derive, from an ordered minimal Gröbner basis, a so-called "minimal Gröbner p-basis" that does have a PLM property. We demonstrate that minimal Gröbner p-bases lend themselves particularly well to derive minimal realization parametrizations over $\mathbb{Z}_{p^r}$. Applications are in coding and sequences over $\mathbb{Z}_{p^r}$.

1 Introduction

Gröbner bases have proved useful tools for dealing with polynomial vectors, with applications particularly in multidimensional system theory. These applications range from controller design to minimal realization of linear systems over fields. Fundamental linear algebraic results on polynomial matrices over fields can be elegantly achieved via the theory of Gröbner bases [1, 4]. In particular, the wellknown Smith-McMillan form as well as the Wiener-Hopf form ("row reducedness") can be achieved. Using the theory of Gröbner bases these are two sides of the same coin, obtained by choosing a different positional term order [11, 23].

In this paper we focus on Gröbner bases for modules of polynomial univariate vector polynomials, i.e., elements of $\mathcal{R}[x]^q$, where q is an integer ≥ 1. In the field case $\mathcal{R} = \mathbb{F}$ all modules are free and a minimal Gröbner basis of a module M is a basis in a linear algebraic sense. It is known that, for certain types of positional term orders, minimal Gröbner bases of modules in $\mathbb{F}[x]^q$ are extremely useful for a range of minimal interpolation-type problems. In this paper we attribute this usefulness to a property that we call the "predictable leading monomial (PLM) property". This property is shared by minimal Gröbner bases in $\mathbb{F}[x]^q$, irrespective of the particular positional term order that is used. In the case that $\mathcal{R}$ is a ring it may happen that a minimal Gröbner basis of a module M in $\mathcal{R}[x]^q$ is not a basis; this may happen even when M is a free module.

*M. Kuijper is with the Department of Electrical and Electronic Engineering, University of Melbourne, VIC 3010, Australia m.kuijper@ee.unimelb.edu.au

†K. Schindelar is with the Lehrstuhl D für Mathematik, RWTH Aachen University Templergraben 64, 52062 Aachen, Germany Kristina.Schindelar@math.rwth-aachen.de

‡This research is partially supported by the Australian Research Council (ARC) and the Deutscher Akademischer Austausch Dienst (DAAD) and co-financed by the Deutsche Forschungsgemeinschaft (DFG)

Motivated by coding applications, we consider modules over the finite ring $\mathbb{Z}_{p^r}$, where p is a prime integer and r is a positive integer. It was shown in [15] that any module M in $\mathbb{Z}_{p^r}[x]^q$ has a particular type of basis, called "reduced p-basis"; [15] gives a constructive procedure that starts from any set of polynomial vectors that generate M. Using Gröbner theory, in this paper we derive an expression for such a reduced p-basis in terms of a minimal Gröbner basis with respect to the TOP (Term Over Position) order. Our result is valid for any choice of positional term order, not just TOP. We show that our p-basis (which we call "minimal Gröbner p-basis") has a PLM property with respect to the chosen positional term order. This PLM property is stronger than the "p-predictable degree property" from [15] and makes minimal Gröbner p-bases ideally suitable for minimal interpolation-type problems, as illustrated in subsection 4.3.

There are several advantages to the Gröbner approach. Firstly, it offers flexibility through the choice of positional term order. This makes it possible to derive several analogous results at once. Secondly, the approach offers scope for extension to other areas where Gröbner bases are a standard tool, such as multidimensional systems. Finally, a third advantage of the Gröbner approach is that computational packages are available to compute minimal Gröbner bases, such as the Singular computer algebra system [10]. A preliminary version of this paper is [16].

2 Preliminaries on Gröbner bases

In this section we present basic notions from Gröbner theory and summarize wellknown results. Most textbooks introduce Gröbner theory in the context of multivariate polynomials, that is, elements of $\mathcal{R}[x_1, \ldots, x_n]$, where $\mathcal{R}$ is a ring. Instead, here we focus on univariate *vector* polynomials, i.e., elements of $\mathcal{R}[x]^q$, where q is an integer ≥ 1. It is wellknown [1, Ex. 4.1.14] that multivariate Gröbner theory can be translated into univariate Gröbner theory for $\mathcal{R}[x]^q$ by using positional monomial orders, such as TOP (Term Over Position) and POT (Position Over Term), defined below, see also [1, sect. 3.5], [2, sect. 10.4], [20, p. 89; p. 104] and the recent survey paper [18]. We focus on properties of Gröbner bases rather than construction of Gröbner bases. For more details on construction the reader is referred to [1, 21, 3].

Throughout this paper $\mathcal{R}$ is assumed to be a noetherian ring, i.e., all its ideals are finitely generated.

The concepts of "degree" and "leading coefficient" for polynomials in $\mathcal{R}[x]$ are extended to polynomial *vectors* in $\mathcal{R}[x]^q$, as follows. Let $\mathrm{e}_1, \ldots, \mathrm{e}_q$ denote the unit vectors in $\mathcal{R}^q$. The elements $x^\alpha \mathrm{e}_i$ with $i \in \{1, \ldots, q\}$ and $\alpha \in \mathbb{N}_0$ are called **monomials**. Several positional term orders can be defined on these monomials; we recall the following two monomial orders (adopting the terminology of [1]):

- The **Term Over Position (TOP)** order, defined as
$$x^\alpha \mathrm{e}_i < x^\beta \mathrm{e}_j \quad :\Leftrightarrow \quad \alpha < \beta \text{ or } (\alpha = \beta \text{ and } i > j).$$
- The **Position Over Term (POT)** order, defined as
$$x^\alpha \mathrm{e}_i < x^\beta \mathrm{e}_j \quad :\Leftrightarrow \quad i > j \text{ or } (i = j \text{ and } \alpha < \beta).$$

Weighted and/or reflected versions of these orders are also possible as in [6]. Clearly, whatever order is chosen, every nonzero element $f \in \mathcal{R}[x]^q$ can be written uniquely as
$$f = \sum_{i=1}^{L} c_i X_i,$$
where $L \in \mathbb{N}$, the c_i's are nonzero elements of $\mathcal{R}$ for $i = 1, \ldots, L$ and the polynomial vectors $X_1, \ldots, X_L$ are monomials, ordered as $X_1 > \cdots > X_L$. Using the terminology of [1] we define

- $\mathrm{lm}(f) := X_1$ as the **leading monomial** of f
- $\mathrm{lt}(f) := c_1 X_1$ as the **leading term** of f
- $\mathrm{lc}(f) := c_1$ as the **leading coefficient** of f

Writing $X_1 = x^{\alpha_1}\, \mathrm{e}_{i_1}$, where $\alpha_1 \in \mathbb{N}_0$ and $i_1 \in \{1, \ldots, q\}$, we define

- $\mathrm{lpos}(f) := i_1$ as the **leading position** of f
- $\deg(f) := \alpha_1$ as the **degree** of f.

Note that for the TOP order the degree of f equals the highest degree of its nonzero components in $\mathcal{R}[x]$, whereas for the POT order it equals the degree of the first nonzero component. Further, for the POT order the leading position of f is the position of the first nonzero component, whereas for the TOP order the leading position of f is the position of the first nonzero component of highest degree.

Below we denote the submodule generated by a polynomial vector f by $\langle f \rangle$. There are several ways to define Gröbner bases, here we adopt the definition of [1] which requires us to first define the concept of "leading term submodule":

Definition 2.1 *Let F be a subset of $\mathcal{R}[x]^q$. Then the submodule $\mathrm{L}(F)$, defined as*

$$\mathrm{L}(F) := \langle \mathrm{lt}(f) \mid f \in F \rangle$$

*is called the **leading term submodule** of F.*

Definition 2.2 *Let $M \subseteq \mathcal{R}[x]^q$ be a module and $G \subseteq M$. Then G is called a **Gröbner basis** of M if*

$$\mathrm{L}(G) = \mathrm{L}(M).$$

It is wellknown [1, Corollary 4.1.17 and Ex. 4.1.14] that a finite Gröbner basis exists for any module in $\mathcal{R}[x]^q$. In general, it can be shown that a Gröbner basis G of a module M generates M, see also Lemma 2.6 below. The following lemma follows immediately from Definition 2.2.

Lemma 2.3 *Let M be a submodule of $\mathcal{R}[x]^q$ with Gröbner basis $G = \{g_1, \ldots, g_m\}$ and let $0 \neq f \in M$. Then there exists a subset $\{g_{j_1}, \cdots, g_{j_s}\}$ of G and $\alpha_1, \ldots, \alpha_s \in \mathbb{N}_0$ and $c_1, \ldots, c_s \in \mathcal{R}$, such that*

- $\mathrm{lm}(f) = x^{\alpha_i}\, \mathrm{lm}(g_{j_i})$ *for $i = 1, \ldots, s$ and*
- $\mathrm{lt}(f) = c_1 x^{\alpha_1}\, \mathrm{lt}(g_{j_1}) + \cdots + c_s x^{\alpha_s}\, \mathrm{lt}(g_{j_s})$.

Note that the g_{j_i}'s of the above lemma all satisfy $\mathrm{lpos}(g_{j_i}) = \mathrm{lpos}(f)$ and $\mathrm{lm}(g_{j_i}) \leq \mathrm{lm}(f)$. The above lemma inspires the next definition.

Definition 2.4 ([1, Def. 4.1.1]) *Let $0 \neq f \in \mathcal{R}[x]^q$ and let $F = \{f_1, \ldots, f_s\}$ be a set of nonzero elements of $\mathcal{R}[x]^q$. Let $\alpha_1, \ldots, \alpha_s \in \mathbb{N}_0$ and let $c_1, \ldots, c_s$ be elements of $\mathcal{R}$ such that*

1. $\mathrm{lm}(f) = x^{\alpha_i}\, \mathrm{lm}(f_i)$ *for $i = 1, \ldots, s$ and*
2. $\mathrm{lt}(f) = c_1 x^{\alpha_1}\, \mathrm{lt}(f_1) + \cdots + c_s x^{\alpha_s}\, \mathrm{lt}(f_s)$.

Define

$$h := f - (c_1 x^{\alpha_1} f_1 + \cdots + c_s x^{\alpha_s} f_s).$$

*Then we say that f **reduces** to h modulo F and we write*

$$f \xrightarrow{F} h.$$

*If f cannot be reduced modulo F, we say that f is **minimal** with respect to F.*

Lemma 2.5 ([1, Lemma 4.1.3]) *Let f, h and F be as in the above definition. If $f \xrightarrow{F} h$ then $h = 0$ or $\text{lm}(h) < \text{lm}(f)$.*

The next lemma is an immediate corollary of Lemma 2.5 that will prove useful in the sequel.

Lemma 2.6 *Let M be a submodule of $\mathcal{R}[x]^q$ with Gröbner basis G and let $0 \neq f \in M$. Then*

$$f \in \langle g \in G \mid \text{lm}(g) \leq \text{lm}(f) \rangle.$$

Definition 2.7 ([1]) *A Gröbner basis G is called **minimal** if all its elements g are minimal with respect to $G \backslash \{g\}$.*

It is known [1, Exercises 4.1.9 & 4.1.14] that a minimal Gröbner basis exists for any module in $\mathcal{R}[x]^q$ and that it has the following convenient property:

Lemma 2.8 *Let $G = \{g_1, \ldots, g_m\}$ be a minimal Gröbner basis. Then $\text{lm}(g_i) \neq \text{lm}(g_j)$ for all $i, j \in \{1, \ldots, m\}$.*

3 The field case

In this section we limit our attention to the case that $\mathcal{R}$ is a field. It is wellknown that Gröbner bases are useful for various applications over fields, including univariate applications. In this section we attribute this usefulness to a particular property of minimal Gröbner bases. We introduce the following terminology.

Definition 3.1 *Let M be a submodule of $\mathcal{R}[x]^q$ and let $F = \{f_1, \ldots, f_s\}$ be a nonempty subset of M. Then F has the **Predictable Leading Monomial (PLM) property** if for any $0 \neq f \in M$, written as*

$$f = a_1 f_1 + \cdots + a_s f_s, \tag{1}$$

where $a_1, \ldots, a_s \in \mathcal{R}[x]$, we have

$$\text{lm}(f) = \max_{1 \leq i \leq s; a_i \neq 0} (\text{lm}(a_i)\, \text{lm}(f_i)). \tag{2}$$

In the Gröbner literature usually a weaker property than the above PLM property is presented, namely: for any f from a module M, generated by $f_1, \ldots, f_s$, there *exist* $a_1, \ldots, a_s \in \mathcal{R}[x]$ such that (1) and (2) hold, see [1, Thm 1.9.1]. In the field case this is clearly equivalent to the PLM property; for this reason the next theorem merely reformulates a wellknown result.

Theorem 3.2 *Let $\mathcal{R}$ be a field. Let M be a submodule of $\mathcal{R}[x]^q$ with minimal Gröbner basis G. Then G has the Predictable Leading Monomial (PLM) property. In particular, G is a basis of M.*

Proof Write $G = \{g_1, \ldots, g_m\}$. Since G is minimal we may assume, by Lemma 2.8, that $\text{lm}(g_1) > \text{lm}(g_2) > \cdots > \text{lm}(g_m)$. Let $f = a_1 g_1 + \cdots + a_m g_m$. For simplicity of notation we assume that a_i is nonzero for $1 \leq i \leq m$. Since $\mathcal{R}$ is a field we have that $\text{lpos}(a_i g_i) = \text{lpos}(g_i)$ for $1 \leq i \leq m$. Also, all leading positions of the g_i's are distinct, otherwise we can reduce. As a result, all leading monomials of the $a_i g_i$'s are distinct. Thus there exist $j_1, \ldots, j_m$, such that

$$\text{lm}(a_{j_1} g_{j_1}) > \text{lm}(a_{j_2} g_{j_2}) > \cdots > \text{lm}(a_{j_m} g_{j_m}).$$

It follows that

$$\text{lm}(f) = \text{lm}(a_{j_1} g_{j_1}) = \text{lm}(a_{j_1})\, \text{lm}(g_{j_1}) = \max_{1 \leq i \leq m} (\text{lm}(a_i)\, \text{lm}(g_i)),$$

which proves the PLM property. Finally, to prove that G is a basis of M, first observe that G generates M by Lemma 2.6. Also, it follows immediately from the PLM property that any nontrivial linear combination of vectors from G has to be nonzero. We conclude that G is a basis of M. $\square$

Note that the PLM property is a strenghtening of the well established predictable degree property from [7, 8], since it involves not only degree information but also leading position information. Also, Theorem 3.2 holds irrespective of the monomial order that is used. Of course, in the field case where all modules are free, the number m of elements in a minimal Gröbner basis equals the dimension of M. The next example demonstrates the usefulness of the PLM property, see also [6].

Example 3.3 *:* **Using minimal Gröbner bases for parametrization of all shortest linear recurrence relations**
Consider the sequence $S_0, S_1, S_2, S_3, S_4 = 1, 4, 3, 3, 2$ *over the field* $\mathbb{Z}_5$*. A polynomial* $d(x)$*, written as* $d(x) = x^L + d_{L-1}x^{L-1} + \cdots + d_1 x + d_0$*, is called a linear recurrence relation of length L for* S_0, S_1, S_2, S_3, S_4 *if*

$$S_{L+j} + \sum_{i=1}^{L} d_{L-i} S_{L+j-i} = 0 \qquad \text{for } j = 0, \ldots, 5 - L - 1. \tag{3}$$

Consider the polynomial $S(x) := S_0x^5 + S_1x^4 + S_2x^3 + S_3x^2 + S_4x$ *and the module* M *spanned by* $\begin{bmatrix} 1 & -S(x) \end{bmatrix}$ *and* $\begin{bmatrix} 0 & x^6 \end{bmatrix}$*. Clearly, any minimal Gröbner basis for* M *must consist of 2 vectors and exactly one of these vectors has leading position* 1*. In fact,* Singular *computes a minimal TOP Gröbner basis* $G = \{g_1, g_2\}$ *for* M*, with* $g_1(x) = \begin{bmatrix} 2x+2 & x^4 - 2x^3 + x \end{bmatrix}$ *and* $g_2(x) = \begin{bmatrix} x^2 - 3x - 1 & 4x^2 - 3x \end{bmatrix}$*. The PLM property of* G *implies that the vector of leading position* 1*, i.e.* g_2*, yields a unique shortest linear recurrence relation, namely* $x^2 - 3x - 1$*. The reader is also referred to the recent paper [17] where Gröbner bases are employed for similar problems.*

Theorem 3.2 does not extend to the case that $\mathcal{R}$ is a ring. At first sight this may seem obvious as there exist modules in $\mathcal{R}[x]^q$ that are not free. Evidently, any minimal Gröbner basis for such a module is not a basis so certainly does not satisfy the PLM property. However, the situation is more subtle: the Gröbner basis of a free module in $\mathcal{R}[x]^q$ is not necessarily a basis either, as we will illustrate in Example 4.15. In this paper we are interested in solving this difficulty for the special case that $\mathcal{R}$ is a ring of the type $\mathbb{Z}_{p^r}$. For this we make use of the special structure of $\mathbb{Z}_{p^r}$.

4 The ring case

4.1 Preliminaries on $\mathbb{Z}_{p^r}$

A set that plays a fundamental role throughout this paper is the set of "digits", denoted by $\mathcal{A}_p = \{0, 1, \ldots, p-1\} \subset \mathbb{Z}_{p^r}$. Recall that any element $a \in \mathbb{Z}_{p^r}$ can be written uniquely as $a = \theta_0 + p\theta_1 + \cdots + p^{r-1}\theta_{r-1}$, where $\theta_\ell \in \mathcal{A}_p$ for $\ell = 0, \ldots, r-1$ (*p-adic expansion*).

Next, adopting terminology from [24], an element a in $\mathbb{Z}_{p^r}$ is said to have **order** k if the additive subgroup generated by a has p^k elements. (Note that [9] and references therein use the terminology **norm** for $r - k$.) Elements of order r are called **units**. Thus the elements $1, p, p^2, \ldots, p^{r-1}$ have orders $r, r-1, r-2, \ldots, 1$, respectively. Let us now choose a monomial order for polynomial vectors in $Z_{p^r}[x]^q$. Given this monomial order, we now extend the above notion of "order" to polynomial vectors as follows.

Definition 4.1 *The **order** of a nonzero polynomial vector* $f \in \mathbb{Z}_{p^r}[x]^q$*, is defined as the order of* $\mathrm{lc}(f)$*, denoted as* $\mathrm{ord}\,(f)$*.*

To deal with the zero divisors occurring in $\mathbb{Z}_{p^r}$ it is useful to use notions of "p-linear dependence" and "p-generator sequence", first introduced for modules in $\mathbb{Z}_{p^r}^q$ in [24]. These notions are based on the p-adic expansion property of $\mathbb{Z}_{p^r}$, which expresses a type of linear independence among the elements 1, p, ..., p^{r-1}. The notions presented below are for *polynomial* vectors; they are extensions of [24], first presented in [15].

Definition 4.2 ([15]) *Let $\{v_1, \ldots, v_N\} \subset \mathbb{Z}_{p^r}[x]^q$. A* ***p*-linear combination** *of $v_1, \ldots, v_N$ is a vector $\sum_{j=1}^{N} a_j v_j$, where $a_j \in \mathbb{Z}_{p^r}[x]$ is a polynomial with coefficients in $\mathcal{A}_p$ for $j = 1, \ldots, N$. Furthermore, the set of all p-linear combinations of $v_1, \ldots, v_N$ is denoted by* ***p*-span**$(v_1, \ldots, v_N)$*, whereas the set of all linear combinations of $v_1, \ldots, v_N$ with coefficients in $\mathbb{Z}_{p^r}[x]$ is denoted by* $\mathrm{span}\,(v_1, \ldots, v_N)$.

Definition 4.3 ([15]) *An ordered sequence $(v_1, \ldots, v_N)$ of vectors in $\mathbb{Z}_{p^r}[x]^q$ is said to be a* ***p*-generator sequence** *if $p\, v_N = 0$ and $p\, v_i$ is a p-linear combination of $v_{i+1}, \ldots, v_N$ for $i = 1, \ldots, N-1$.*

Theorem 4.4 ([15]) *Let $v_1, \ldots, v_N \in \mathbb{Z}_{p^r}[x]^q$. If $(v_1, \ldots, v_N)$ is a p-generator sequence then*

$$p\text{-}\mathrm{span}\,(v_1, \ldots, v_N) = \mathrm{span}\,(v_1, \ldots, v_N).$$

In particular, $p\text{-}\mathrm{span}\,(v_1, \ldots, v_N)$ is a submodule of $\mathbb{Z}_{p^r}[x]^q$.

All submodules of $\mathbb{Z}_{p^r}[x]^q$ can be written as the p-span of a p-generator sequence. In fact, if $M = \mathrm{span}\,(g_1, \ldots, g_m)$ then M is the p-span of the p-generator sequence

$$(g_1, pg_1, \ldots, p^{r-1}g_1, g_2, pg_2, \ldots, p^{r-1}g_2, \ldots, g_m, pg_m, \ldots, p^{r-1}g_m).$$

Definition 4.5 ([15]) *The vectors $v_1, \ldots, v_N \in \mathbb{Z}_{p^r}[x]^q$ are said to be* ***p*-linearly independent** *if the only p-linear combination of $v_1, \ldots, v_N$ that equals zero is the trivial one.*

Definition 4.6 ([15, 13]) *Let M be a submodule of $\mathbb{Z}_{p^r}[x]^q$, written as a p-span of a p-generator sequence $(v_1, \cdots, v_N)$. Then $(v_1, \cdots, v_N)$ is called a* ***p*-basis** *of M if the vectors $v_1, \ldots, v_N$ are p-linearly independent in $\mathbb{Z}_{p^r}[x]^q$. The number of elements of a p-basis is called the* ***p*-dimension** *of M, denoted as $p\text{-}\dim\,(M)$.*

The following definition adjusts the PLM property, introduced for the field case in Definition 3.1, to the specific structure of $\mathbb{Z}_{p^r}$.

Definition 4.7 *Let M be a submodule of $\mathbb{Z}_{p^r}[x]^q$ and let $F = \{f_1, \ldots, f_s\}$ be a nonempty subset of M. Then F has the* ***p*-Predictable Leading Monomial (*p*-PLM) property** *if for any $0 \neq f \in M$, written as*

$$f = a_1 f_1 + \cdots + a_s f_s, \tag{4}$$

where $a_1, \ldots, a_s \in \mathcal{A}_p[x]$, we have

$$\mathrm{lm}(f) = \max_{1 \le i \le s;\, a_i \neq 0} (\mathrm{lm}(a_i)\, \mathrm{lm}(f_i)).$$

Note that in the above definition $a_i \in \mathcal{A}_p[x]$ rather than $a_i \in \mathcal{R}[x]$ as in Definition 3.1. Further note that multiplications and additions in (4) are over $\mathbb{Z}_{p^r}$; also observe that $\mathcal{A}_p[x]$ is not closed under addition, for example, in $\mathbb{Z}_4[x]$, we have $x \in \mathcal{A}_2[x]$ but $x + x = 2x \notin \mathcal{A}_2[x]$.

4.2 Main result

By Lemma 2.8, a minimal Gröbner basis $G = \{g_1, \ldots, g_m\}$ has the convenient property that its elements can be ordered so that $\mathrm{lm}(g_1) > \cdots > \mathrm{lm}(g_m)$ since their leading monomials are distinct. Unlike the field case, a minimal Gröbner basis of a module in $\mathbb{Z}_{p^r}[x]^q$ is, in general, *not* a basis. In fact, the leading positions of its elements are not necessarily distinct. This may happen even when the module is free. We have the following lemma.

Lemma 4.8 *Let M be a submodule of $\mathbb{Z}_{p^r}[x]^q$ with minimal Gröbner basis $G = \{g_1, \ldots, g_m\}$, ordered so that $\mathrm{lm}(g_1) > \cdots > \mathrm{lm}(g_m)$. Let $j < i$ be such that $\mathrm{lpos}(g_j) = \mathrm{lpos}(g_i)$. Then $\deg g_j > \deg g_i$ and $\mathrm{ord}\ (g_j) > \mathrm{ord}\ (g_i)$. In particular, $m \leq qr$.*

Proof Since $\mathrm{lpos}(g_j) = \mathrm{lpos}(g_i)$ and $\mathrm{lm}(g_j) > \mathrm{lm}(g_i)$ we must have that $\deg(g_j) > \deg(g_i)$, regardless of the monomial order that is used. It then follows that $\mathrm{ord}\ (g_j) > \mathrm{ord}\ (g_i)$, otherwise g_j could be reduced by g_i and this would contradict the fact that G is a minimal Gröbner basis. This proves the main result of the lemma. Since there are only r values of $\mathrm{ord}\ (g_i)$ possible, it also follows that $m \leq qr$. □

As a result of the previous lemma we can define a sequence of "order differences" as follows.

Definition 4.9 *Let M be a submodule of $\mathbb{Z}_{p^r}[x]^q$ with minimal Gröbner basis $G = \{g_1, \ldots, g_m\}$ ordered so that $\mathrm{lm}(g_1) > \cdots > \mathrm{lm}(g_m)$. For $1 \leq j \leq m$ define*

$$\beta_j := \mathrm{ord}\ (g_j) - \mathrm{ord}\ (g_i),$$

where i is the smallest integer $> j$ with $\mathrm{lpos}(g_i) = \mathrm{lpos}(g_j)$. If i does not exist we define $\beta_j := \mathrm{ord}\ (g_j)$. The sequence $(\beta_1, \ldots, \beta_m) \in \mathbb{N}^m$ is called the ***sequence of order differences*** *of G.*

The next theorem shows that the natural ordering of elements of a minimal Gröbner basis yields a particular p-generator sequence. Note that the theorem holds for any choice of monomial order.

Theorem 4.10 *Let M be a submodule of $\mathbb{Z}_{p^r}[x]^q$ with minimal Gröbner basis $G = \{g_1, \ldots, g_m\}$, ordered so that $\mathrm{lm}(g_1) > \cdots > \mathrm{lm}(g_m)$. Let $(\beta_1, \ldots, \beta_m)$ be the sequence of order differences of G as per Definition 4.9. Then*

$$(g_1, pg_1, \cdots, p^{\beta_1 - 1}g_1, g_2, pg_2, \cdots, p^{\beta_2 - 1}g_2, \cdots, g_m, pg_m, \cdots, p^{\beta_m - 1}g_m) \tag{5}$$

is a p-generator sequence whose p-span equals M.

Proof We first prove that (5) satisfies Definition 4.3. By definition $\beta_m = \mathrm{ord}\ (g_m)$, so that

$$\mathrm{lm}(p^{\beta_m} g_m) < \mathrm{lm}(g_m). \tag{6}$$

Suppose $p^{\beta_m} g_m \neq 0$, then according to Lemma 2.3 there exists $g_i \in G$ such that $\mathrm{lm}(g_i) \leq \mathrm{lm}(p^{\beta_m} g_m)$. But then (6) implies that $\mathrm{lm}(g_i) < \mathrm{lm}(g_m)$ which contradicts $\mathrm{lm}(g_1) > \cdots > \mathrm{lm}(g_m)$. We conclude that

$$p^{\beta_m} g_m = 0. \tag{7}$$

To prove that (5) satisfies Definition 4.3 it now obviously remains to prove that $p^{\beta_j} g_j$ is a p-linear combination of

$$g_{j+1}, pg_{j+1}, \ldots, p^{\beta_{j+1}-1}g_{j+1}, g_{j+2}, pg_{j+2}, \ldots, p^{\beta_{j+2}-1}g_{j+2}, \ldots, g_m, \ldots, p^{\beta_m - 1}g_m \tag{8}$$

for $1 \leq j \leq m-1$. For this, we first prove that $p^{\beta_j} g_j$ is a linear combination of $g_{j+1}, g_{j+2}, \ldots, g_m$. We distinguish two cases:
<u>case I</u>

$\beta_j = \operatorname{ord} g_j$. Then $\operatorname{lm}(p^{\beta_j} g_j) < \operatorname{lm}(g_j)$, so that, by Lemma 2.6, $p^{\beta_j} g_j$ is a linear combination of $g_{j+1}, g_{j+2}, \ldots, g_m$.

case II

$\beta_j < \operatorname{ord} g_j$, so that $\operatorname{lm}(p^{\beta_j} g_j) = \operatorname{lm}(g_j)$. By definition, there exists a smallest integer $i > j$ with $\operatorname{lpos}(g_i) = \operatorname{lpos}(g_j)$ and $\beta_j = \operatorname{ord}(g_j) - \operatorname{ord}(g_i)$. Observe that then $\operatorname{ord}(p^{\beta_j} g_j) = \operatorname{ord}(g_i)$ and $\deg(p^{\beta_j} g_j) = \deg(g_j) > \deg(g_i)$ (use Lemma 4.8), whereas $\operatorname{lpos}(p^{\beta_j} g_j) = \operatorname{lpos}(g_j) = \operatorname{lpos}(g_i)$. Thus we can find $a \in Z_{p^r}[x]$ such that $\operatorname{lt}(p^{\beta_j} g_j) = \operatorname{lt}(a g_i)$. As a result, $\operatorname{lm}(p^{\beta_j} g_j - a g_i) < \operatorname{lm}(p^{\beta_j} g_j) = \operatorname{lm}(g_j)$. Consequently, by Lemma 2.6, $p^{\beta_j} g_j - a g_i$ is a linear combination of $g_{j+1}, g_{j+2}, \ldots, g_m$. Since $i > j$ it follows that $p^{\beta_j} g_j$ is also a linear combination of $g_{j+1}, g_{j+2}, \ldots, g_m$.

Thus for $1 \le j \le m-1$

$$p^{\beta_j} g_j \text{ is a linear combination of } g_{j+1}, \ldots, g_m. \tag{9}$$

Finally, we prove by induction that (8) holds for $1 \le j \le m-1$. For $j = m-1$ this follows from (7) and the fact that $p^{\beta_{m-1}} g_{m-1}$ is a multiple of g_m because of (9). Now suppose that (8) holds for $j = j_0 \in \{1, \ldots, m-1\}$. Consider the vector $p^{\beta_{j_0-1}} g_{j_0-1}$. By (9) there exist $a_{j_0}, \ldots, a_m \in \mathbb{Z}_{p^r}[x]$ such that

$$p^{\beta_{j_0-1}} g_{j_0-1} = a_{j_0} g_{j_0} + \cdots + a_m g_m.$$

Now use the p-adic decomposition to write

$$a_{j_0} = a_{j_0}^0 + p a_{j_0}^1 + \cdots + p^{r-1} a_{j_0}^{r-1},$$

where $a_{j_0}^i \in \mathcal{A}_p[x]$ for $0 \le i \le r-1$. Repeatedly using the induction hypothesis it follows that

$$p^{\beta_{j_0-1}} g_{j_0-1} = a_{j_0}^0 g_{j_0} + p\text{-linear combination of } g_{j_0+1}, \ldots, g_m.$$

This proves that (8) holds for $j = j_0 - 1$, so that, by induction, (5) is a p-generator sequence.

To prove that its p-span equals M, we first note that, by Lemma 2.6, any element of M can be written as a linear combination of $g_1, g_2, \ldots, g_m$. Using a similar reasoning as above this can be alternatively written as a p-linear combination of the vectors in (8). $\square$

The next lemma follows immediately from Definition 4.9.

Lemma 4.11 *Let M be a submodule of $\mathbb{Z}_{p^r}[x]^q$ with minimal Gröbner basis $G = \{g_1, \ldots, g_m\}$, ordered so that $\operatorname{lm}(g_1) > \cdots > \operatorname{lm}(g_m)$. Let $(\beta_1, \ldots, \beta_m)$ be the sequence of order differences of G as per Definition 4.9 and let $N = \beta_1 + \beta_2 + \cdots + \beta_m$. Let $(v_1, \ldots, v_N)$ be the p-generator sequence given by (5). Then for any $i, j \in \{1, \ldots, N\}$ with $i \neq j$ we have*

$$\operatorname{lpos}(v_i) = \operatorname{lpos}(v_j) \Rightarrow \operatorname{ord}(v_i) \neq \operatorname{ord}(v_j).$$

The next theorem is the ring analogon of Theorem 3.2 and presents the main result of this section.

Theorem 4.12 *Let M, $(\beta_1, \ldots, \beta_m)$ and $\{v_1, \ldots, v_N\}$ be defined as in the previous lemma. Then $\{v_1, \ldots, v_N\}$ has the p-PLM property.*
In particular, $(v_1, \ldots, v_N)$ is a p-basis of M so that

$$N = p\text{-}\dim(M) = \beta_1 + \beta_2 + \cdots + \beta_m.$$

Proof Let

$$f = a_1 v_1 + \cdots + a_N v_N \tag{10}$$

with $a_1, \ldots, a_N \in \mathcal{A}_p[x]$. For simplicity of notation we assume that a_i is nonzero for $1 \le i \le N$. Let us first examine two special cases:

Special case I

All g_i's have distinct leading positions. Then the proof is analogous to the field case, i.e., the proof of Theorem 3.2.

Special case II

All g_i's have the same leading position. Then all v_i's also have the same leading position. By Lemma 4.11 their orders are all different. Now observe that $\mathrm{ord}(a_i v_i) = \mathrm{ord}(v_i)$ for $1 \le i \le N$ since $a_i \in \mathcal{A}_p[x]$. Thus all $a_i v_i$'s have different orders. In particular, all $a_i v_i$'s of largest degree have different orders, so that their leading coefficients add up to a nonzero element of $\mathbb{Z}_{p^r}$ (use the p-adic decomposition). This implies that the p-PLM property holds.

Let us now consider the general case. By grouping together all vectors $a_i v_i$ of the same leading position we write

$$f = f_1 + f_2 + \cdots + f_q,$$

where $f_i = 0$ if position i is not used in (10). As in Special case II above it can be shown that $\mathrm{lpos}(f_i) = i$ whenever $f_i \neq 0$. As a result, the nonzero f_i's can be ordered and it follows that

$$\mathrm{lt}(f) = \mathrm{lt}(f_j) \tag{11}$$

for some nonzero f_j with $j \in \{1, \ldots, q\}$. Recall that f_j is defined as the sum of all vectors in the right hand side of (10) that have leading position j. It now follows from Special case II above that there exists $\ell \in \{1, \ldots, N\}$ such that $\mathrm{lm}(f_j) = \mathrm{lm}(a_\ell)\,\mathrm{lm}(v_\ell)$. As a result, by equation (11),

$$\mathrm{lm}(f) = \mathrm{lm}(a_\ell)\,\mathrm{lm}(v_\ell). \tag{12}$$

Evidently $\mathrm{lm}(f) \le \max_{1 \le i \le N; a_i \neq 0}(\mathrm{lm}(a_i)\,\mathrm{lm}(v_i))$, so that (12) implies that equality holds. This proves the p-PLM property.

Finally, to prove that $(v_1, \ldots, v_N)$ is a p-basis for M, first observe that p-span $(v_1, \ldots, v_N) = M$ by Theorem 4.10. Also, it follows immediately from the p-PLM property that any nontrivial p-linear combination of vectors in $\{v_1, \ldots, v_N\}$ has to be nonzero. We conclude that $(v_1, \ldots, v_N)$ is a p-basis of M, so that $N = p{-}\dim\,(M) = \beta_1 + \beta_2 + \cdots + \beta_m$. □

Remark 4.13 *We stress the difference between the above p-PLM property and the property of a so-called "strong Gröbner basis" G in the literature (terminology from [19]) which states that for any* $f \in M$ *there* exist $a_1, \ldots, a_m \in \mathbb{Z}_{p^r}[x]$ *such that* $\mathrm{lm}(f) = \max_{1 \le i \le m; a_i \neq 0}(\mathrm{lm}(a_i)\,\mathrm{lm}(g_i))$, *see also [1, Thm 4.1.12], as well as [19] and [5, Th. 2.4.3]. In the terminology of [9], this is formulated as "any* $f \in M$ *possesses an H-presentation relative to G". In the Gröbner basis literature it seems to be generally accepted that uniqueness of representation via Gröbner bases can not be obtained for the ring case. However, in this paper we adopt the novel approach of [15] of restricting coefficients to* $\mathcal{A}_p[x]$ *to achieve the p-PLM property, which implies uniqueness of representation.*

Definition 4.14 *Let M be a submodule of $\mathbb{Z}_{p^r}[x]^q$ with minimal Gröbner basis $G = \{g_1, \dots, g_m\}$, ordered so that $\mathrm{lm}(g_1) > \cdots > \mathrm{lm}(g_m)$. Let $(\beta_1, \dots, \beta_m)$ be the sequence of order differences of G as per Definition 4.9. Let $(v_1, v_2, \dots, v_N)$ be the p-generator sequence given by (5). Then $(v_1, v_2, \dots, v_N)$ is called a* **minimal Gröbner p-basis** *for M.*

Example 4.15 *Let M be a submodule of $\mathbb{Z}_9^2[x]$, given as $M =$ span $\{s_1, s_2\}$, where $s_2(x) = \begin{bmatrix} 0 & x^6 \end{bmatrix}$ and $s_1(x) = [1 \quad -S(x)]$ with $S(x) := x^5 + 4x^4 + 4x^3 + 7x^2 + 7x$.*

- *Using the* TOP *order:*
  a minimal Gröbner basis $G = \{g_1, \dots, g_4\}$ of M is given by the rows of

$$\begin{bmatrix} 8 & \underline{x^5} + 4x^4 + 4x^3 + 7x^2 + 7x \\ x+5 & \underline{3x^4} + 3x^2 + x \\ \underline{x^2} + 3x + 2 & x^2 + 4x \\ \underline{3x} + 6 & 3x \end{bmatrix}.$$

  Note that M is a free module but G is not a basis. The sequence of order differences $(\beta_1, \beta_2, \beta_3, \beta_4)$ equals $(1, 1, 1, 1)$. By Theorem 4.12, the sequence (g_1, g_2, g_3, g_4) is a minimal Gröbner p-basis for M and therefore has the p-PLM property. Furthermore, $p-\dim(M) = \beta_1 + \beta_2 + \beta_3 + \beta_4 = 4$.

- *Using the* POT *order:*
  in this case the vectors s_1 and s_2 constitute a minimal Gröbner basis that happens to be a basis for M. The sequence of order differences (β_1, β_2) equals $(2, 2)$. According to Theorem 4.12, the sequence $(s_1, 3s_1, s_2, 3s_2)$ is a minimal Gröbner p-basis for M; it has the p-PLM property. In fact, $\{s_1, s_2\}$ has the PLM property as per Definition 3.1. Note that $\beta_1 + \beta_2$ equals $4 = p-\dim(M) = 2\dim(M)$, as expected.

Note that in this example the number of elements of the minimal POT Gröbner basis differs from the number of elements of the minimal TOP Gröbner basis, something that can't happen in the field case. However, the example clearly illustrates a corollary of Theorem 4.12, namely that the sum of the β_i's is an invariant of the module M, namely $N = p-\dim(M)$. Any minimal Gröbner p-basis of M must consist of N vectors, no matter which monomial order is used. Further, note that if the TOP order is used then a minimal Gröbner p-basis is a "reduced p-basis" in the terminology of [15]. Indeed, the p-PLM property clearly implies the p-predictable degree property of [15]. Thus one of the applications where a minimal TOP Gröbner p-basis can be used is in convolutional coding over $\mathbb{Z}_{p^r}$: a minimal TOP Gröbner p-basis then serves as a minimal p-encoder of a convolutional code over $\mathbb{Z}_{p^r}$ in the terminology of [12, 13]. Applications for which the p-PLM property is particularly useful are parametrizations for minimal interpolation-type problems, as illustrated in the next subsection.

4.3 An application over $\mathbb{Z}_{p^r}$

In the previous subsection we introduced the novel concept of "minimal Gröbner p-basis" for modules over $\mathbb{Z}_{p^r}$. In this subsection we put this concept to work to get a particularly transparent derivation of a parametrization of all shortest linear recurrence relations of a finite sequence over $\mathbb{Z}_{p^r}$ that parallels the one in [14]. In particular, we demonstrate the usefulness of the p-PLM property.

Consider the sequence $S_0, S_1, \dots, S_{n-1}$ over $\mathbb{Z}_{p^r}$. We call a polynomial $f \in \mathbb{Z}_{p^r}[x]$, written as $f(x) = f_L x^L + f_{L-1}x^{L-1} + \cdots + f_1 x + f_0$, a **linear recurrence relation** of length L for $S_0, \dots, S_{n-1}$ if f_L is a unit and

$$f_L S_{L+j} + \sum_{i=1}^{L} f_{L-i} S_{L+j-i} = 0 \qquad \text{for } j = 0, \dots, n-L-1. \tag{13}$$

As usual, we call the polynomial f **monic** if $f_L = 1$. As in Example 3.3, define the polynomial $S(x)$ as

$$S(x) := S_0 x^n + S_1 x^{n-1} + \cdots + S_{n-1} x, \tag{14}$$

and consider $M = \text{ span } \{s_1, s_2\}$, where $s_1(x) = \begin{bmatrix} 1 & -S(x) \end{bmatrix}$ and $s_2(x) = \begin{bmatrix} 0 & x^{n+1} \end{bmatrix}$. Obviously, M is a free module for which $\{s_1, s_2\}$ is a minimal POT Gröbner basis with $(\beta_1, \beta_2) = (r, r)$. Clearly, $\{s_1, s_2\}$ is even a basis for M and $p-\dim\ (M) = 2r$. The theorem below parallels Theorem 15 of [14], where Gröbner bases are not used; note that here no reordering of p-basis vectors is required because the natural order of a minimal Gröbner p-basis suffices.

Theorem 4.16 *Let $S(x) = S_0 x^n + S_1 x^{n-1} + \cdots + S_{n-1} x \in \mathbb{Z}_{p^r}[x]$ and let*

$$M = \text{ span } \{\begin{bmatrix} 1 & -S(x) \end{bmatrix}, \begin{bmatrix} 0 & x^{n+1} \end{bmatrix}\}.$$

Let $(v_1, v_2, \ldots, v_{2r})$ be a minimal TOP Gröbner p-basis of M, with v_i written as $v_i = [d_i \quad -h_i] \in \mathbb{Z}^2_{p^r}[x]$ for $i = 1, \ldots, 2r$. Let $\ell \in \{1, \ldots, 2r\}$ be such that $\text{lpos}(v_\ell) = 1$ and $\text{ord}\ (v_\ell) = r$. Then d_ℓ is a shortest linear recurrence relation for the sequence $S_0, \ldots, S_{n-1}$. Furthermore, a parametrization of all shortest linear recurrence relations for $S_0, \ldots, S_{n-1}$ is given by

$$q_\ell d_\ell + \sum_{i>\ell} q_i d_i, \tag{15}$$

with $0 \neq q_\ell \in \mathcal{A}_p$ and $q_i \in \mathcal{A}_p[x]$ with $\deg q_i \leq \deg v_\ell - \deg v_i$ for $i = \ell + 1, \ldots, 2r$.

Proof We use a behavioral setup as in [14]. Consider the *partial impulse response behavior*

$$\mathcal{B} := \text{ span } \{\boldsymbol{b}, \sigma\boldsymbol{b}, \sigma^2\boldsymbol{b}, , \ldots, \sigma^n\boldsymbol{b}\},$$

where $\boldsymbol{b}$ is defined as

$$\boldsymbol{b} = \left(\begin{bmatrix} S_0 \\ 0 \end{bmatrix}, \begin{bmatrix} S_1 \\ 0 \end{bmatrix}, \ldots, \begin{bmatrix} S_{n-1} \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \ldots \right).$$

It is easily verified that $M = \mathcal{B}^\perp$, that is, M consists of all annihilators of $\mathcal{B}$. As a result, v_ℓ is an annihilator of $\mathcal{B}$, that is,

$$[d_\ell(\sigma) \quad -h_\ell(\sigma)]\,\boldsymbol{w} = 0$$

is a kernel representation whose behavior includes $\mathcal{B}$. Also $\deg\ h_\ell \leq \deg\ d_\ell$. It then follows immediately that d_ℓ is a linear recurrence relation for $S_0, \ldots, S_{n-1}$.
Next, suppose that a polynomial $d^\star \in \mathbb{Z}_{p^r}[x]$ is a shortest linear recurrence relation for $S_0, \ldots, S_{n-1}$. Then there exists a polynomial $h^\star \in \mathbb{Z}_{p^r}[x]$ of degree $\leq \deg\ d^\star$ such that $[d^\star \quad -h^\star] \in M$. Since $(v_1, v_2, \ldots, v_{2r})$ is a minimal Gröbner p-basis of M we can write $[d^\star \quad -h^\star]$ as a p-linear combination of $v_1,\ v_2 \ldots, v_{2r}$. Since v_ℓ is the unique vector in this TOP Gröbner p-basis of leading position 1 and order r, this p-linear combination *must* use v_ℓ. Because of the p-PLM property of $\{v_1, \ldots, v_N\}$ (Theorem 4.12), it follows that $\deg\ d^\star \geq \deg\ v_\ell$. This implies that v_ℓ is a *shortest* linear recurrence relation for $S_0, \ldots, S_{n-1}$. Moreover, it also follows from the p-PLM property of $\{v_1, \ldots, v_N\}$ that the above p-linear combination can *not* use v_i for $i < \ell$. This proves the parametrization (15). $\square$

Example 4.17 Consider the sequence $S_0, S_1, S_2, S_3, S_4 = 1, 4, 4, 7, 7$ over the ring $\mathbb{Z}_9$. Let M be the submodule of $\mathbb{Z}_9^2[x]$, defined as in Theorem 4.16. As shown in Example 4.15, a minimal TOP Gröbner p-basis $G = \{g_1, g_2, g_3, g_4\}$ is given by the rows of

$$\begin{bmatrix} 8 & \underline{x^5} + 4x^4 + 4x^3 + 7x^2 + 7x \\ x+5 & \underline{3x^4} + 3x^2 + x \\ \underline{x^2} + 3x + 2 & x^2 + 4x \\ \underline{3x} + 6 & 3x \end{bmatrix}.$$

According to Theorem 4.16, g_3 gives a shortest linear recurrence relation x^2+3x+2; a parametrization of all shortest linear recurrence relations is given by

$$(\Theta_1(x^2 + 3x + 2) + (\Theta_2 x + \Theta_3)(3x + 6),$$

where $(\Theta_i \in \{0, 1, 2\}$ for $i = 1, 2, 3$; $\Theta_1 \neq 0$. It is easily seen that a parametrization of all *monic* shortest linear recurrence relations is given by

$$x^2 + 3x + 2 + \Theta(3x + 6),$$

where $(\Theta \in \{0, 1, 2\}$, which concurs with [14]. Note that this example illustrates that non-uniqueness occurs despite the fact that the complexity is less than $(n + 1)/2$, a situation that does not occur in the field case.

Example 4.18 Consider the sequence $S_0, S_1, S_2, S_3, S_4 = 6, 3, 1, 5, 6$ over the ring $\mathbb{Z}_9$, as in [22]. The iterative algorithm of [22] computes a shortest linear recurrence relation $x^3 + 4x^2 + 7x + 1$; note that no parametrization is given in [22]. Here we demonstrate how a minimal TOP Gröbner p-basis can be used to derive a parametrization. For this, let M be the submodule of $\mathbb{Z}_9^2[x]$, defined as in Theorem 4.16. SINGULAR computes the minimal TOP Gröbner basis $G = \{g_1, g_2\}$ of M, where $g_1 = \begin{bmatrix} x^3 + 4x^2 + 7x + 4 & x^2 + 3x \end{bmatrix}$ and $g_2 = \begin{bmatrix} 6x^2 + 8 & x^3 + 5x^2 + 6x \end{bmatrix}$. Note that, unlike Example 4.17, G is a basis for M. According to Theorem 4.12, the sequence $(g_1, 3g_1, g_2, 3g_2)$ is a minimal TOP Gröbner p-basis for M. According to Theorem 4.16, g_1 gives a shortest linear recurrence relation $x^3 + 4x^2 + 7x + 4$; a parametrization of all monic shortest linear recurrence relations is given by

$$x^3 + 4x^2 + 7x + 4 + \Theta_1(6x^2 + 8) + 6\Theta_2,$$

where $\Theta_i \in \{0, 1, 2\}$ for $i = 1, 2$. Thus for $\Theta_1 = 0$ and $\Theta_2 = 1$ we recover the shortest linear recurrence relation $x^3 + 4x^2 + 7x + 1$ from [22]. In fact, G has the PLM property as per Definition 3.1 and the above parametrization can be rewritten as

$$x^3 + 4x^2 + 7x + 4 + \Theta(6x^2 + 8),$$

where $\Theta \in \mathbb{Z}_9$. For $\Theta = 3$ we recover the shortest linear recurrence relation $x^3 + 4x^2 + 7x + 1$ from [22].

Note that both Example 4.17 and Example 4.18 are concerned with a free module. The two examples differ in the sense that G is a basis in Example 4.18 but not a basis in Example 4.17. This situation does not happen in the field case, where any minimal Gröbner basis of a module is a basis. In Example 4.17 G happens to be a p-basis that has the p-PLM property, whereas in Example 4.18 G happens to be a basis that has the PLM property. In general, modules in $\mathbb{Z}_{p^r}[x]^q$ may have a minimal Gröbner basis that is neither a basis nor a p-basis. Our main result Theorem 4.12 shows how to construct a p-basis from G that has the p-PLM property.

5 Conclusions

The main contributions of the paper are twofold. Firstly, we identified a particularly useful property, that we labeled the "Predictable Leading Monomial (PLM)" property. A generating set of a module M in $\mathcal{R}[x]^q$ that has this property is necessarily a basis for M. For the case that $\mathcal{R}$ is a field the PLM property is shared by minimal Gröbner bases of any module in $\mathcal{R}[x]^q$. This is not necessarily the case when $\mathcal{R}$ is a ring, even when the module is free. As our second main contribution, for any module M in $\mathcal{R}[x]^q$, we showed how to derive a particular set from a minimal Gröbner basis G of M. We called this set a "minimal Gröbner p-basis" of M and showed that it has a so-called "p-PLM property". The result is fairly trivial if G happens to be a basis. However, the result is non-trivial in case G is not a basis. We illustrated the latter with an example of a free module in $\mathbb{Z}_9[x]^2$. To demonstrate the usefulness of the p-PLM property, we showed how to obtain a parametrization of all shortest linear recurrence relations of a finite sequence over $\mathbb{Z}_{p^r}$ from a minimal TOP Gröbner p-basis of a particular free module. Such parametrizations can be exploited to decode beyond the minimum distance of Reed-Solomon codes, i.e., for list decoding, see the recent paper [25]. Similarly, parametrizations of interpolating solutions can be obtained for list decoding of Reed-Solomon codes.

One of the advantages of the Gröbner approach is its flexibility in the choice of monomial order. This not only makes it possible to derive several analogous results at once, but also makes it possible to relate results obtained for different monomial orders. For example, in the linear recurrence application we made use of the fact that a minimal POT Gröbner p-basis of a module M has the same number of elements as a minimal TOP Gröbner p-basis of M. A possible topic of future research is a Smith-McMillan like canonical form for polynomial matrices over $\mathbb{Z}_{p^r}$. This is motivated by issues concerning catastrophicity of convolutional codes over $\mathbb{Z}_{p^r}$, see [13].

The approach lends itself well to generalization to the multivariate case, see also [9] and references therein. This is another possible topic of future research.

Acknowledgment

We thank one of the anonymous reviewers for detailed and helpful comments that have improved the clarity of the paper.

References

[1] W. W. Adams and P. Loustaunau. *An introduction to Gröbner Bases*, volume 3 of *Graduate Stud. Math.* American Mathematical Society, 1994.

[2] T. Becker and V. Weispfenning. *Gröbner bases.* Springer-Verlag, 1993.

[3] M. Brickenstein, A. Dreyer, G. M. Greuel, M. Wedler, and O. Wienand. New developments in the theory of Gröbner bases and applications to formal verification. *Special Issue of the Journal of Pure and Applied Algebra*, submitted.

[4] B. Buchberger. Gröbner bases: A short introduction for systems theorists. In *Computer Aided Systems Theory EUROCAST 2001*, volume 2178/2008 of *Lecture Notes in Computer Science*, pages 1–19. Springer Berlin / Heidelberg, 2001.

[5] E. Byrne and P. Fitzpatrick. Gröbner bases over Galois rings with an application to decoding alternant codes. *J. Symbolic Comput.*, 31:565–584, 2001.

[6] P. Fitzpatrick. On the key equation. *IEEE Trans. Inf. Th*, 41:1290–1302, 1995.

[7] G.D. Forney. Convolutional codes I: Algebraic structure. *IEEE Trans. Inf. Th*, 16:720–738, 1970. ;correction, vol. IT-17, p.360, 1971.

[8] G.D. Forney, Jr. Minimal bases of rational vector spaces, with applications to multivariable linear systems. *SIAM J. Control*, 13:493–520, 1975.

[9] E.V. Gorbatov. Standard basis of a polynomial ideal over commutative Artinian chain ring. *Discrete Math. Appl.*, 14:75–101, 2004.

[10] G. M. Greuel, G. Pfister, and H. Schrönemann. SINGULAR 3.0.4, *a computer algebra system for polynomial computations*. Centre for Computer Algebra, University of Kaiserslautern, 2005. `http://www.singular.uni-kl.de`.

[11] M. Avelino Insua Hermo. *Varias perspectives sobre las bases de Gröbner: forma normal de Smith, algorithme de Berlekamp y algebras de Leibniz*. PhD thesis, Universidade de Santiago de Compostela, 2005.

[12] M. Kuijper and R. Pinto. Minimal trellis construction for finite support convolutional ring codes. In A. Barbero, editor, *Coding Theory and Applications (ICMCTA)*, LN in Computer Science 5228, pages 95–106. Springer, 2008.

[13] M. Kuijper and R. Pinto. On minimality of convolutional ring encoders. *IEEE Trans. Inf. Th.*, IT-55:4890–4897, 2009.

[14] M. Kuijper and R. Pinto. Parametrization of linear recurrence relations by row reduction for sequences over a finite ring. In *Proc. 18th International Symposium on Mathematical Theory of Networks and Systems (MTNS)*, pages 1–12, Virginia Tech, USA, July 2008.

[15] M. Kuijper, R. Pinto, and J. W. Polderman. The predictable degree property and row reducedness for systems over a finite ring. *Linear Algebra and its Applications*, 425:776–796, 2007.

[16] M. Kuijper and K. Schindelar. Gröbner bases and behaviors over finite rings. In *Proceedings of 48th IEEE Conf. Decision and Control (CDC'09)*, pages 8101–8106, Shanghai, China, December 2009.

[17] K. Lee and M.E. O'Sullivan. List decoding of Reed-Solomon codes from a Gröbner basis perspective. *J. Symbolic Comput.*, 43:645–658, 2008.

[18] Z. Lin, L. Xu, and N. K. Bose. A tutorial on Gröbner bases with applications in signals and systems. *IEEE Transactions on circuits and systems*, 55:445–461, 2008.

[19] G. Norton and A. Salagean. Cyclic codes and minimal strong Gröbner bases over a principal ideal ring. *Finite Fields and their Applications*, 9:237–249, 2003.

[20] U. Oberst. Multidimensional constant linear systems. *Acta Applicandae Mathematicae*, 20:1–175, 1990.

[21] F. Pauer. Gröbner bases with coefficients in rings. *J. Symbolic Comput.*, 42:no. 11–12, 1003–1011, 2007.

[22] J.A. Reeds and N.J.A. Sloane. Shift-register synthesis (modulo m). *SIAM J. Computing*, 14:505–513, 1985.

[23] K. Schindelar and V. Levandovskyy. Computing normal forms using Gröbner bases. submitted (March 2009) to Journal of Symbolic Computation.

[24] V.V. Vazirani, H. Saran, and B.S. Rajan. An efficient algorithm for constructing minimal trellises for codes over finite abelian groups. *IEEE Trans. Inf. Th.*, 42:1839–1854, 1996.

[25] Y. Wu. New list decoding algorithms for Reed-Solomon and BCH codes. *IEEE Trans. Inf. Th.*, 54:3611–3630, 2008.